# Hackback in Deutschland: Wer, was, wie und warum?

Dennis-Kenji Kipker 2019-06-03T20:53:40

Ende Mai ergaben Recherchen des Bayerischen Rundfunks, dass die Bundesregierung das schon seit Längerem diskutierte Thema „Hackback“ (oder auch „aktive Cyberabwehr“) nunmehr politisch offensiv angeht: So liegt ein internes Konzeptpapier vor, das den behördlichen Abstimmungsprozess nach einem „erheblichen Cyber-Angriff aus dem Ausland“ beschreibt. Geplant ist dabei wohl, nach einem vierstufigen Raster mit Gegenmaßnahmen unterschiedlicher Intensität vorzugehen: Die ersten beiden Stufen sollen den schadhaften Datenverkehr lediglich blockieren oder umleiten. Sie stellen noch keinen digitalen Gegenschlag im Sinne des „Hackback“ dar. Anders sieht es auf den folgenden Stufen aus: Auf der dritten Stufe sollen Behörden fremde Netze aktiv infiltrieren dürfen, um Daten zu verändern oder zu löschen. Die vierte Stufe sieht Maßnahmen vor, die nicht nur Daten oder Software, sondern auch Hardware betreffen können. Beispielhaft werden in dem Bericht das „Eindringen in Systeme“ und das „Herunterfahren“ genannt. Es liegt jedoch nahe, dass sich staatliche Gegenmaßnahmen nicht allein darauf beschränken müssen.

## Neue Herausforderungen für die Cyber-Sicherheit – neue Strategien für die Cyber-Sicherheit

Zuvorderst sei festgestellt: Dass in der gegenwärtigen technischen und politischen Situation das Thema „Hackback“ durch die Bundesregierung aufgegriffen wird, ergibt durchaus Sinn, denn die mediale Berichterstattung der vergangenen Jahre hat verdeutlicht, dass Maß und Zahl von Cyber-Angriffen zugenommen haben. Zudem gibt es stetig mehr Akteure, die im digitalen Raum aus den unterschiedlichsten Motiven heraus tätig werden und sowohl Staat als auch Wirtschaft kompromittieren. Die jährlich veröffentlichten Lageberichte des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bestätigen diese Tendenz. Darüber hinaus legt die Cyber-Sicherheitsstrategie der Bundesregierung aus 2016 fest, dass aktiv Maßnahmen zu ergreifen sind, um das Niveau der IT-Sicherheit in Deutschland und Europa ganzheitlich zu verbessern. Angefangen mit dem IT-Sicherheitsgesetz aus 2015 und gefolgt vom aktuellen Referentenentwurf des IT-SiG 2.0, wird eine Vielzahl durchaus sinnvoller Maßnahmen zur IT-Sicherheit in die Gesetzgebung eingebracht, für die – im Gegensatz zu so mancher staatlicher Überwachungstechnologie – tatsächlich ein Bedarf besteht. Die EU geht mit ihrer neuen Cyber-Sicherheitsstrategie aus 2017 und dem jüngst vom EP verabschiedeten Cybersecurity Act in eine ähnliche Richtung ganzheitlicher IT-Sicherheit. Dass innerhalb dieses regulatorischen Milieus auch über „Hackbacks“ gesprochen wird, ist deshalb erst einmal nachvollziehbar.

# Zuständigkeitswirrwarr für Hackbacks?

Wie aber können „Hackbacks“ von einer politischen Blaupause in konkrete Pläne und Maßnahmen transferiert werden? Aus dem internen Konzeptpapier, das dem BR vorliegt, geht bereits ein zentrales Problem hervor: Wer ist in Deutschland für die Durchführung der „Hackbacks“ zuständig, welche Behörde besitzt die rechtlichen und technischen Kompetenzen, um hier tätig zu werden? Eine zentrale Rolle spielt dabei das bereits existierende Nationale Cyber-Abwehrzentrum (NCAZ), das vereinfacht gesprochen eine Informations- und Kooperationsplattform für all jene Behörden ist, die das Thema Cyber-Sicherheit bearbeiten. Hier kommen das BSI, das Bundesamt für Verfassungsschutz (BfV), der Militärische Abschirmdienst (MAD), der Bundesnachrichtendienst (BND), das Bundeskriminalamt (BKA), das Zollkriminalamt (ZKA), die Bundespolizei (BPol) und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zusammen – eine Vielzahl unterschiedlicher Zuständigkeiten an einem Ort, die ein ganzheitliches Lagebild der Cyber-Sicherheit erarbeiten sollen. Im NCAZ soll letztlich auch entschieden werden, ob ein „erheblicher Cyber-Angriff aus dem Ausland“ vorliegt, der einen „Hackback“ evoziert. Sobald in fachlicher Hinsicht grünes Licht für einen Gegenangriff gegeben wird, soll ein weiteres Gremium, bestehend aus Vertretern des Kanzleramts, des AA, des BMJV, des BMVg und des BMI die Aktion in politischer Hinsicht bestätigen. Im Konzeptpapier heißt es sodann, dass vornehmlich der BND für die Durchführung des „Hackbacks“ geeignet sei, denn er „bewege sich unter anderem in IT-Infrastrukturen im Ausland, sammelt konstant Informationen über Cyberangreifer, deren Vorgehen und Infrastrukturen und wertet diese detailliert aus“. Es soll daneben wohl auch möglich sein, dass eine Polizeibehörde den „Hackback“ übernimmt, und der BND für diesen Fall „zwingend“ einbezogen wird.

In rechtlicher Hinsicht ist es aber fraglich, ob die Zuständigkeit zur Durchführung der „Hackbacks“ tatsächlich vorrangig beim BND liegen sollte. Auch dass trotz des Trennungsgebots zwischen Polizei und Nachrichtendiensten beide zusammenwirken sollen, um „Hackbacks“ durchzuführen, erscheint fragwürdig. Der BND hat als Nachrichtendienst gem. § 1 Abs. 2 BNDG vornehmlich die Aufgabe, solche Informationen, die zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die BRD sind, zu sammeln und auszuwerten. Diese Aufgabenregelung, auf Fragen der Cyber-Sicherheit angewandt, bedeutet, dass der BND zwar umfassende Informationen über relevante Daten sammeln, aber nicht selber aktive Cyber-Angriffe durchführen darf, was beim „Hackback“ aber der Fall wäre. Auch ist die Abgrenzung zum Tätigkeitsbereich des Verfassungsschutzes für Fragen der Cyber-Sicherheit nicht immer leicht zu klären. Dessen Aufgaben werden in § 3 BVerfSchG konkretisiert: Nach den Nr. 1 und 2 sammelt und wertet die Behörde solche Informationen aus, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten gegen die BRD für eine fremde Macht betreffen, oder solche Bestrebungen umfassen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane zum Ziel haben. Beide Tatbestände können zwar durch unzulässige Cyber-Interventionen erfüllt sein, aus den Aufgabenzuweisungen ergibt sich aber, dass der Verfassungsschutz eben

vornehmlich im Inland, und der BND vornehmlich im Ausland tätig wird. Letztlich dürfte aber im Falle (ausländischer) Cyberattacken oft die Situation vorliegen, dass sich in- und ausländische Interessenkreise überschneiden. Auch das BSI und das BKA dürften unabhängig von ihren fachlichen Kompetenzen gegenwärtig nicht die richtigen Ansprechpartner sein, wenn es um Hackbacks geht: Das BSI ist zumindest zurzeit noch ausschließlich für die Aufrechterhaltung und Förderung der operativ-technischen IT-Sicherheit und zur Zusammenarbeit mit Staat und Wirtschaft zuständig. Aktiv geführte technische Angriffe, die Einrichtungen im Ausland betreffen und diese im Zweifelsfall kompromittieren oder zerstören sollen, fallen nicht in seine Zuständigkeit. Das BKA ist vornehmlich eine Strafverfolgungsbehörde, die zwar Computerdelikte ermitteln kann und soll, aber nicht selbst Cyber-Angriffe im Ausland durchführt. Für die BPol stellen sich ähnliche Probleme, wenn es um das Tätigwerden im Ausland geht. Darüber hinaus dürfte sich bei den verschiedenen anderen Behörden des NCAZ die Frage stellen, ob gleichermaßen auch eine technische Kompetenz vorliegt, aktive „Hackbacks“ zu realisieren.

## Ein alter Bekannter: Die Bundeswehr

Die Besonderheit – und damit die rechtliche Crux – beim Thema „Hackback“ liegt darin, dass die Zuständigkeitsabgrenzungen mit der grenzüberschreitenden Natur und der Vielzahl von Interessen und Akteuren bei Cyber-Angriffen verschwimmen. Wo befinden wir uns im Bereich der Prävention, wann beginnt die Gefahrenabwehr, was sind die Anforderungen an repressive Handlungen? Und nicht zuletzt auch die Frage: Sind „Hackbacks“ in das Ausland überhaupt als klassische nachrichtendienstliche, polizeiliche oder repressive Maßnahmen zu qualifizieren? Einiges spricht dafür, dass dem nicht so ist – womit wir wieder beim altbekannten Thema „Bundeswehr und Cyber-Angriff“ wären. Die Diskussion, die hierzu in den letzten Jahren geführt wurde, ist genauso umfassend wie fruchtlos. Mit dem „Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr“ wurde 2016 eine grundlegende Strategie erarbeitet, wie ein Tätigwerden der Bundeswehr im digitalen Raum, dem so genannten „Cyber- und Informationsraum“ (CIR), aussehen könnte. Für den CIR wurde im April 2017 ein eigenes „Kommando Cyber- und Informationsraum“ (KdoCIR) in Dienst gestellt. Innerhalb des KdoCIR existiert seit 2018 das Zentrum Cyberoperationen (ZCO), das technische Kapazitäten vorsieht, die auch in der Lage sind, Offensivmaßnahmen im digitalen Raum, also theoretisch „Hackbacks“, durchzuführen. Bei gegebenen technischen Kapazitäten stellt sich folglich die Frage, unter welchen rechtlichen Voraussetzungen die Bundeswehr hier tätig werden könnte.

Und spätestens hier dürfte es wirklich problematisch werden, denn ein Tätigwerden der Bundeswehr im CIR setzt voraus, dass die hohen verfassungsrechtlichen Hürden für den Einsatz deutscher Streitkräfte erfüllt sind. Zentral ist hier der Art. 87a GG, der vorschreibt, dass die Streitkräfte außer zur Verteidigung nur dann eingesetzt werden dürfen, soweit es das Grundgesetz ausdrücklich zulässt. Der Ausnahmevorbehalt ist eng zu lesen und betrifft vornehmlich Situationen des inneren Notstands oder überregionale Unglücksfälle. Der Einsatz der Bundeswehr zum „Hackback“ setzt folglich einen Verteidigungsfall voraus, und das bedeutet die Reaktion auf eine militärische Gewaltanwendung, die

von außen kommt. Dieses Kriterium wird für den im Konzeptpapier skizzierten Regelfall des „Hackback“-Szenarios nicht erfüllt sein. Außerdem dürfte für die Entscheidung zur Durchführung einer Cyber-Operation der Bundeswehr nicht das im Konzeptpapier skizzierte politische Entscheidungsgremium befugt sein, sondern allein der Bundestag. Offensivmaßnahmen der Bundeswehr im CIR, die nicht unter das Selbstverteidigungsrecht fallen, sind zudem völkerrechtswidrig, da sie das Gewaltverbot missachten. Nicht umsonst gehen auch die Überlegungen fehl, allgemein einen NATO-Bündnisfall für Cyberattacken anzunehmen, da diese vielfach nicht die Schwelle zu einem bewaffneten Angriff überschreiten.

Im Ergebnis ist deshalb festzustellen: Ja, es kann in technischer Hinsicht durchaus sinnvoll sein, auch aktive Maßnahmen zur Cyber-Sicherheit zu ergreifen, soweit eine gewisse Erheblichkeitsschwelle überschritten ist. Hierzu können auch „Hackbacks“ gehören. In rechtlicher Hinsicht kann diese Nützlichkeit aber nicht überspielen, dass „Hackbacks“ keine erheblichen Cyber-Angriffe sein dürfen, die letztlich einer militärischen Operation gleichkommen. Auch ist fraglich, ob Nachrichtendienste hier die richtigen Akteure sind, da ihre eigentliche Aufgabe in der Sammlung und Auswertung von Informationen besteht. Da es sich bei „Hackbacks“ auch um Maßnahmen handelt, die das operative „Alltagsgeschäft“ der Cyber-Sicherheit betreffen, sollte das BSI noch stärker als bisher in diese Aufgabe einbezogen werden, zumal der Entwurf für ein IT-SiG 2.0 bereits eine ähnliche Richtung einschlägt. Dies betrifft natürlich nur solche Vorgänge, die einen originären Bezug auch zu inländischen Sachverhalten aufweisen.

---